DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

SECNAVINST 3501.1A
DON CIO
16 Dec 2005

SECNAV INSTRUCTION 3501.1A

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY (DON) CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Ref: (a) Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization and Protection, of 17 Dec 03
(b) Presidential Decision Directive/PDD-63, Critical Infrastructure Protection, of 22 May 98
(c) The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets, Feb 03
(d) The National Strategy to Secure Cyberspace, Feb 03
(e) Federal Preparedness Circular 65, of 15 Jun 04
(f) Homeland Security Presidential Directive/HSPD-5, Management of Domestic Incidents, of 28 Feb 03
(g) DOD Directive 3020.40, Defense Critical Infrastructure Program (DCIP), of 19 Aug 05
(h) SECNAVINST 5000.2C, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, of 19 Nov 04
(i) DOD Directive 3020.26, Defense Continuity Program, of 8 Sep 04
(j) DON Consequence Management (CM) Planning Guide, Second Ed, 6 Oct 04
(k) SECNAVINST 5430.7N, Assignment of Responsibilities and Authorities in the office of the Secretary of the Navy, of 9 Jun 05
(l) SECNAVINST 3030.4A, Department of the Navy Continuity of Operations (DON COOP) Program, of 27 Jul 04
(m) DON Remediation Planning Guide, First Ed, 25 Jun 04

Encl: (1) Critical Infrastructure Protection Definitions
(2) Department of the Navy Critical Infrastructure Protection Council Members
(3) Department of the Navy Critical Infrastructure Protection Working Group

1. Purpose. This instruction provides revised policy and delineates specific responsibilities for implementing Critical Infrastructure Protection in the Department of the Navy (DON). This instruction has been administratively revised and should be reviewed in its entirety.

2. Cancellation. SECNAVINST 3501.1 upon promulgation and effective date of this instruction. This instruction contains significant revisions and should be reviewed in its entirety.

3. Applicability and Scope. This directive applies to the Offices of the Secretary of the Navy, the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all Navy and Marine Corps activities, installations, and commands.

4. Definitions. CIP terminology is defined in enclosure (1).

5. Background. Reference (a) supersedes portions of reference (b), Presidential Decision Directive/NSC 63 of 22 May 98 (PDD-63), and updates our national intent to identify, prioritize, assess, remediate, and coordinate the protection of our critical infrastructures and key resources. However, PDD-63 remains the authority for establishing the Critical Infrastructure Assurance Officer (CIAO) in Federal Departments and Agencies. References (c) through (f) provide national strategic policy and guidance regarding protection of physical and cyber infrastructures as well as domestic incident management and consequence management planning. Reference (g) is the Department of Defense (DOD) policy for protection of the Defense Infrastructure. It requires all DOD components to have a comprehensive and effective Defense Continuity Program that ensures DOD Component Mission Essential Functions (MEFs) continue under all circumstances across the spectrum of threats.

6. Policy. DON CIP complements and helps ensure mission assurance. Protection of the Department’s critical infrastructures requires participation by all hands to identify potential vulnerabilities, defend against exploitation, and if exploited, minimize the impact to overall mission. CIP embraces traditional aspects of security (Anti-Terrorism/Force Protection, Operational Security, Physical Security, Information and Infrastructure Assurance). As such, CIP supports overall

mission assurance by linking assets, especially certain critical assets, to DON missions. There are six CIP life cycle phases:

- Infrastructure Analysis and Assessment
- Remediation
- Indications and Warning (I&W) for the Intelligence community/Monitoring and Reporting (M&R) for the CIP community
- Mitigation
- Response
- Reconstitution

These phases span activities that occur before, during, and after natural or man-made events, which may result in infrastructure compromise or disruption. A key aspect of CIP is recognizing the relationships and the importance of DON assets and installations with critical infrastructures that support Regional and Combatant Commander (COCOM) requirements, particularly Operations Plans (OPLANs). It is therefore DON policy to:

a. Identify, assess and protect physical and cyber infrastructures deemed critical to DON force and materiel readiness and operations in peace, crisis, and war; mitigate the effect of their loss or disruption; and/or plan for timely restoration or recovery.

b. Recognize that DON equipment, facilities, utilities, services, weapon systems, as well as intangible assets supporting mission accomplishment are highly dependent upon non-DON assets, including national or international infrastructures, facilities and services of the private sector, defense industrial base (DIB), and other government departments and agencies. DON, as well as non-DON, assets critical to mission assurance may be intangible, such as unique skill sets, intellectual property and key business processes.

c. Observe, report, and propose action required for the protection of non-DON infrastructures and assets whose security is primarily with the private and non-military asset owners and with local, state, and federal law enforcement authorities;

including non-United States infrastructures and assets that are the responsibility of appropriate foreign and national authorities for protection.

d. Increase the awareness of the CIP program and the role of DON personnel within the program through information sharing, cooperative agreements and outreach with the private sector, education partnerships, state and local government partnerships, exchange of personnel, training and education, and other efforts.

e. Consider CIP a critical element in acquisition and operations planning.

f. Institutionalize CIP within the Department through endorsing educational curricula, outreach, “best practices” and “lessons learned” to create a fundamental cultural change concerning the importance of the DOD and DON CIP programs to mission assurance.

g. Determine the risk to mission critical systems and processes supporting organic and non-organic assets. Non-organic infrastructures and services that serve as sole source producers or single nodes of vulnerability in delivery and operational sustainment of Acquisition Category I through IV weapons systems, or any other critical acquisition programs, shall be considered. Acquisition management procedures shall be modified to incorporate requirements for the identification, prioritization, and protection of defense critical infrastructure in acquisition, maintenance and sustainment contracts in accordance with references (g) and (h).

h. Use the results of the various analyses performed under the CIP program, such as the risk analysis and business impact analysis, along with an approved risk management methodology to determine needed funding, and to obtain management approval of resources and actions for effecting changes in business practices or procedures to protect critical infrastructures or assets.

i. Conduct integrated Consequence Management (CM) planning across the DON in accordance with references (e) and (i). Reference (j) provides additional consequence management planning guidance to sustain Mission Essential Functions against

all-hazard disruptions.

j. Establish a DON CIP Council to oversee the overnance, implementation and execution of CIP within the Department. Enclosure (2) is the DON CIP Council membership. The DON CIP Council shall:

(1) Convene as directed by the DON CIAO.

(2) Determine the necessary efforts to institutionalize CIP implementation and protection improvements throughout the Department of the Navy to ensure warfighter mission assurance.

(3) Monitor progress of CIP throughout the Department, making policy change recommendations, and directing appropriate actions to support the Navy and Marine Corps team effort in ensuring the mission assurance of the Combatant Commanders in the execution of the National Military Strategy.

(4) Seek to foster CIP cooperation and collaboration within the Department and in CIP matters with DOD and other Federal authorities to improve CIP effectiveness.

(5) Contribute subject matter expertise to support the Office of the Secretary of Defense (OSD) sector CIAOs.

(6) Identify resource sponsors and asset owners responsible for DON critical infrastructures.

(7) Recommend resource actions to support CIP implementation, remediation and continued mission assurance through protection of DON critical assets and associated infrastructures.

k. Establish a DON CIP Working Group to coordinate CIP implementation among stakeholders within the Department. Enclosure (3) is the DON CIP Working Group membership. The DON CIP Working Group shall:

(1) Be comprised of senior subject matter experts at the O-5/6 or civilian equivalent grade.

(2) Meet as needed in support of continuing CIP developments; report progress to, and receive direction from, the DON CIP Council.

(3) Determine the necessary efforts to institutionalize CIP implementation and protection improvements throughout the Department of the Navy to ensure warfighter mission assurance.

(4) Facilitate CIP cooperation and collaboration within the Department and in CIP matters with DOD and other federal authorities to improve CIP effectiveness.

(5) Recommend resource actions to support CIP implementation, remediation and continued mission assurance through protection of DON critical assets and associated infrastructures.

(6) Provide input to support future CIP policy.

(7) Assist COCOMs and regional asset owners as needed in identifying critical infrastructures to be assessed in existing and future IVA processes.

7. Responsibilities

a. The Department of the Navy Chief Information Officer (DON CIO) shall serve as the Department of the Navy Critical Infrastructure Assurance Officer (DON CIAO) (See references (b) and (k)) and shall:

(1) Represent the Secretary (when the Secretary or Under Secretary are not available) on senior DON CIP or Critical Infrastructure Assurance panels, boards, meetings and conferences.

(2) Provide appropriate membership to senior DOD and Homeland Defense Critical Infrastructure Protection, Critical Infrastructure Assurance panels, boards, meetings and conferences.

(3) Oversee DON CIP initiatives and coordinate activities with the Secretariat, CNO and CMC as appropriate.

(4) Chair the DON Critical Infrastructure Protection

Council (enclosure (2)) and conduct meetings as needed, but at a minimum of once annually, to share findings, concerns, and best practices from DON entities involved with or responsible for mission assurance efforts.

(5) Make CIP an integral factor in DON CIO policies.

(6) Serve as the overall manager and central point of contact for DON CIP related issues. This includes, but is not limited to: actions taken to establish, and execute an organizational program supporting the DCIP; collaborating with appropriate entities; establishing and maintaining a secure database of DON critical assets; monitoring remediation efforts; promoting visibility and support for programmatic and budgetary expenditures; and maintaining active liaison with other existing CIP-related programs in DOD, the federal government, and industry to establish and promulgate CIP policy and share best practices and seek economies in efforts required to assess and remediate assets (government and commercial owned) that are critical to DON warfighting readiness.

(7) Provide guidance as appropriate to the DON CIP Working Group.

(8) Develop information-sharing strategies for CIP initiatives, using web based as well as existing tools and processes. Promulgate guidance for DON entities on key CIP issues, including developing integrated continuity of operations plans and procedures, ensuring consistency with existing DON, DOD, and federal policy as well as best practices.

(9) Develop new, or leverage existing, CIP related tools and guidance, including self-assessment and risk management tools and provide them to asset owners.

(10) Coordinate with DON activities as well as DOD, for the identification of DON critical assets. Conduct periodic updates to reflect changes in technology, infrastructure, as well as DOD and DON requirements.

(11) Direct policy, monitor and provide oversight guidance for an Integrated Vulnerability Assessment (IVA)

program closely coordinated with both Services including the existing CNO (N3IPS) and CMC (Code PP&O) IVA processes; computer network defense assessment capabilities resident in Navy Information Operations Command (NIOC) and Marine Corps Network Operations & Security Command (MCNOSC); non-organic and organic mission dependencies analysis and assessment as specified by DON CIAO; disaster preparedness and consequence management, continuity of operations plans assessments and reviews; and other mission-focused critical infrastructure assessment protocols as required to assess potential vulnerabilities to mission assurance, incorporating at every opportunity lessons learned from previous assessments and DOD, DON and industry best practices. Compile and assess trends identified during vulnerability assessments and apply to overarching guidance products and tools.

(12) Capture DON critical assets, IVA results, remediation status and other related imagery and data into a critical asset management system to support focused intelligence, situational awareness, and decision-making. Publish and coordinate data sharing requirements for other supporting Department systems. Coordinate and facilitate data sharing with DOD, DON and other supported systems using a critical asset management system as the DON system of record.

b. The Assistant Secretary of the Navy, (Research, Development and Acquisition) (ASN (RD&A)) shall:

(1) Serve as a member of the DON CIP Council.

(2) Provide a senior acquisition community subject matter expert to the DON CIP Working Group. This representative shall be knowledgeable and familiar with the Secretary of Defense (OSD) CIP Industrial Sector Working Group issues. This individual will also represent the DON to the USD (AT&L).

(3) Work with the DON CIAO to identify, characterize, prioritize, and remediate vulnerabilities to critical non-organic infrastructures and processes managed by the acquisition community.

(4) Review policies that may be affected by CIP consideration and revise as necessary, making CIP an integral factor in policies directing RD&A actions.

(5) Require CIP consideration in acquisition management procedures to incorporate requirements for the identification, prioritization, and protection of defense critical infrastructure in the life cycle of acquisition programs. References (b) and (h) pertain.

c. The Assistant Secretary of the Navy (Financial Management and Comptroller) (ASN(FM&C)) shall:

(1) Serve as a member of the DON CIP Council.

(2) Provide a senior Financial Sector subject matter expert to the DON CIP Working Group. This representative shall be knowledgeable and familiar with the DFAS-led OSD CIP Financial Sector Working Group issues.

(3) Be responsible for the oversight of DON critical financial infrastructures and develop CIP sensitive procedures for remediation, mitigation, and assurance that the minimum essential level of financial operations can be protected and maintained.

(4) Work with the other CIP sectors, as required, in addressing security requirements of DON financial infrastructures.

(5) Review policies that may be affected by CIP consideration and revise as necessary, making CIP an integral factor in policies directing FM&C actions.

d. The Assistant Secretary of the Navy (Installations and Environment) (ASN(I&E)) shall:

(1) Serve as a member of the DON CIP Council.

(2) Provide senior subject matter expert knowledgeable in public works and environmental issues to the DON CIP Working Group. It is critical to the DON CIP Working Group that this representative be knowledgeable and familiar with the U.S. Army Corps of Engineers-led OSD CIP Public Works Sector Working Group.

(3) Integrate CIP in the review of plans and policies that may be affected by CIP consideration to include privatization, strategic sourcing, and Public-Private Ventures (PPV), and make CIP an integral factor in policies directing I&E actions, including directing facilities and utilities planning, design, construction, and maintenance.

e. The Assistant Secretary of the Navy (Manpower and Reserve Affairs) (ASN(M&RA)) shall:

(1) Serve as a member of the DON CIP Council.

(2) Provide a senior DON Personnel Sector subject matter expert to the DON CIP Working Group. This individual shall be knowledgeable and familiar with OSD CIP Personnel sector issues. This individual will represent the DON to the OSD CIP Personnel sector working group.

(3) Be responsible for the oversight of DON critical personnel infrastructures and develop CIP sensitive procedures for remediation, mitigation, and assurance that the minimum essential level of operations can be protected and maintained.

(4) Review policies that may be affected by CIP consideration and revise as necessary, making CIP an integral factor in policies directing M&RA actions.

f. The Director, Naval Criminal Investigative Service (NCIS) shall:

(1) Serve as a member of the DON CIP Council, and provide a representative to the DON CIP Working Group in the areas of assessment and Indications and Warning (I&W).

(2) In partnership with the Office of Naval Intelligence (ONI), coordinate with DON CIAO in developing a comprehensive Indications and Warning capability of threats to critical infrastructures from unconventional sources (i.e., Foreign Intelligence Services, terrorism, etc.).

(3) Continue to lead CNO (N3IPS) Integrated Vulnerability Assessments.

(4) Assist in the identification of CIP weaknesses and vulnerabilities and the development of remediation strategies.

(5) Review policies that may be affected by CIP consideration and revise as necessary, making CIP an integral factor in policies directing NCIS actions and programs.

(6) Continue to support a critical asset management. system in the Multi-Threat Alert Center (MTAC) as a decision support database for providing intelligence analysts with DON critical asset information and as a tool to develop focused threat intelligence information.

g. The General Counsel (OGC) shall:

(1) Serve as a member of the DON CIP Council and provide legal counsel in support of CIP efforts.

(2) Review policies that may be affected by CIP consideration and revise as necessary, making CIP an integral factor in policies directing actions and programs.

h. The Naval Inspector General shall:

(1) Serve as a member of the DON CIP Council.

(2) Participate as a contributor to the DON CIP Working Group.

(3) Evaluate and report, the incorporation and implementation of DON CIP policy within Navy commands.

i. The Deputy Naval Inspector General for Marine Corps Matters shall:

(1) Serve as a member of the DON CIP Council.

(2) Participate as a contributor to the DON CIP Working Group.

(3) Evaluate and report, the incorporation and implementation of DON CIP policy within Marine Corps commands.

j. The CNO and CMC shall:

(1) Be responsible for CIP Program execution and attendant directions within their respective Service(s), and when directed, identify and document assets and critical infrastructures.

(2) Contribute leadership on the DON CIP Council per enclosure (2).

(3) Provide senior subject matter experts familiar with sector issues to the DON CIP Working Group per enclosure (3).

(4) Implement DON CIP policy to ensure mission assurance for the Navy and Marine Corps.

(5) Advise the DON CIAO on policy recommendations for CIP.

(6) Incorporate CIP into appropriate training programs.

(7) Work with the DON CIAO and the DON CIP Council to ensure the remediation of identified vulnerabilities to critical infrastructures and assets are given appropriate consideration in planning, programming, budgeting, and execution (PPBE).

(8) In order to monitor and further institutionalize CIP within the Department of the Navy, establish Critical Infrastructure Protection measures of performance to monitor program progress for CIP areas of interest, such as: Anti-Terrorism Force Protection; Computer Network Defense; Consequence Management; and Commercial Dependency. Measures of performance should be developed in coordination with the DON CIAO, not later than ninety days from the date of promulgation of this instruction, and should address policy, programmatic and budgetary expenditures, future plans, impediments to success, lessons learned, and best practices.

(9) Ensure every shore-based command formally appoints a CIP point of contact to facilitate CIP coordination throughout the chain of command.

(10) Ensure that all commands have documented and implemented continuity of operations (COOP) plans that provide the means to continue DON mission essential functions during all disruptive events in accordance with reference (l).

(11) Assess vulnerabilities to critical systems and assets per reference (g) using, as appropriate, DON tools and guides. (See references (j) and (m))

(12) In conjunction with the DON CIAO, establish an enterprise-wide risk management plan to determine the maximum level of acceptable risk to identified critical infrastructures and assets, based on their contribution to war fighting mission and system vulnerability.

(13) Keep DON CIAO advised of coordination efforts with appropriate COCOM, DOD and DON Infrastructure Sector managers as to the prioritization of critical infrastructure vulnerabilities, the associated risk, and remediation. Except for measures clearly unique to a tenant's mission, the host shall exercise general authority over tenants for coordination of CIP issues.

(14) Provide, when required, for Navy and Marine Corps subordinate commands: local plans for CIP remediation (See reference (i)); local plans for response and mitigation; CIP tabletop and actual exercise plans, and local CIP best practices.

(15) Keep the DON CIAO advised of degradation, damage, or loss of DON Critical Assets and mission essential functions, and their recovery and reconstitution as a matter of DON mission assurance to DOD.

(16) Conduct, test and exercise integrated planning in accordance with reference (l) to sustain organizational Mission Essential Functions against all-hazard disruptions.

(17) Review policies that may be affected by CIP consideration and revise as necessary making CIP an integral factor in policies directing actions and programs.

8. Action. This instruction is effective immediately.

D. M. Wennergren
Department of the Navy
Chief Information Officer

Distribution:
Electronic only, via Navy Directives Website
http://neds.daps.dla.mil//

Glossary of Department of the Navy Critical Infrastructure Protection Definitions

Assessment (Critical Infrastructure Protection). (1) Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. (2) Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 1-02) (3) An assessment is an objective evaluation of the vulnerabilities associated with Joint Force Capabilities. (4) Objective determination of how critical the capability and supporting infrastructure is in supporting military operations that accomplish the National Military Strategy. Focus is Combatant Command Operations Plans. (5) A process to characterize the Department of Defense (DOD) infrastructures, their dependencies and interdependencies and subsequent linkages to commercial, foreign and host nation infrastructures.

Asset (Infrastructure). A distinguishable entity that provides a service or capability. Assets are people, physical entities or information located either within or outside the United States and owned or operated by domestic foreign, public or private sector organizations. (DOD Directive 3020.40 of 19 Aug 2005)

Assurance (Critical Capability/Infrastructure). Assurance is guarding against the loss or disruption of a critical capability/infrastructure. Assurance assumes the identification of capabilities, assets, nodes, and infrastructures deemed critical to the Department of Defense in peacetime, crisis and war. Assurance requires assessing potential threats and identifying potential actions to restore those capabilities, assets, nodes, and infrastructures (or functionality they provide) if they are lost, damaged, corrupted, or compromised. Further, assurance requires identifying and resourcing options to protect, mitigate, and improve the availability of these Critical Capabilities and Infrastructures that DOD organizations own, use, and control.

The goal of assurance is to inform planners and decision makers of the probability of availability and quality (e.g., integrity, reliability, confidentiality, survivability, endurability, capacity, adequacy) of specific capabilities and infrastructures. Examples of assurance activities are dedication of physical

protection resources, development of redundant capability/means, alter OPLANS and Contingency Plans (CONPLANS) that depend on the identified capability or accept risk and do nothing. Assurance of a Critical Capability and/or Infrastructure is a shared responsibility.

Capability. The ability to execute a specified course of action. (Joint Publication (JP) 1-02)

Consequence Management. Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. Also called CM. (JP 3-26 and JP 1-02). The technique used to maintain continuity of operations. How a command manages the consequences of an event directly impacts its ability to maintain continuity of operations. (Department of the Navy Critical Infrastructure Protection Consequence Management Planning Guide, Second Edition, 6 Oct 2004)

Continuity of Operations (COOP). An internal effort within individual components of the Executive, Legislative, and Judicial Branches of Government assuring the capability exists to continue uninterrupted essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack-related emergencies. COOP involves plans and capabilities covering the same functional objectives of Continuity of Government (COG), must be maintained at a high level of readiness, and be capable of implementation both with and without warning. COOP is not only an integral part of COG and Enduring Constitutional Government (ECG), but is simply "good business practice" - part of the Department of Defense's fundamental mission as a responsible and reliable public institution. (DOD Directive 3020.26 of 8 Sep 2004)

Critical Asset. (1) A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (JP 3-26 and JP 1-02). (2) An asset of such extraordinary importance to Department of Defense (DOD) operations in peace, crisis and war that its incapacitation or destruction would have a very

serious, debilitating effect on the ability of the Department of Defense to fulfill its missions. (DOD Directive 3020.40 of 19 Aug 2005)

Critical Asset List (CAL). A compilation of infrastructure items determined to be essential to the execution of directed mission responsibilities.

Critical Asset Management System (CAMS). The repository (data base) for DON Critical Infrastructure Assets. CAMS functions as the Authoritative Data Source for threat analysis against mission critical infrastructure for Senior DON CIP decision makers.

Critical Infrastructure. The facilities, systems, and functions that comprise our critical infrastructures are highly sophisticated and complex. They include human assets and physical and cyber systems that work together in processes that are highly interdependent. They also consist of key nodes that, in turn, are essential to the operation of the critical infrastructures in which they function.

Critical Infrastructure Assurance Officer (CIAO). The CIAO is responsible for the protection of all of the department's critical infrastructures. The CIAO shall establish procedures for obtaining expedient and valid authority to allow vulnerability assessments to be performed on computer and physical systems. The Department of the Navy CIAO is the Department of the Navy Chief Information officer, who was initially appointed by Under Secretary of the Navy memorandum of 26 Aug 1999 (NOTAL), and chairs the DON Critical Infrastructure Protection Council. (SECNAVINST 5430.7N of 9 Jun 2005)

Critical Infrastructure Protection (CIP). (1) Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc. (DODD 3020.40, 19 Aug 2005) (2) The identification, assessment, and security of physical and cyber systems and assets so vital to the Nation that their incapacitation or destruction would have a debilitating impact on national security, national economic

security, and/or national public health and safety. Within the Department of Defense, it is the identification, assessment, and security enhancement of physical and cyber assets and associated infrastructures essential to the execution of the National

Military Strategy. Defense CIP is a complementary program linking the mission assurance aspects of Anti-Terrorism, Force Protection, Information Assurance, Continuity of Operations (COOP), and Readiness programs. (JP 3-26 and DOD Directive 3020.26 of 8 Sep 2004) (3) Proactive risk management actions intended to prevent or deter a threat from attempting to, or succeeding at, destroying or incapacitating critical infrastructures.

Critical Infrastructure Protection Council. Council comprised of senior civilian leadership, Flag and General Officers who support the DON CIAO in decision making and leadership for Critical Infrastructure Protection in the Department of the Navy. (SECNAVINST 3501.1A of 16 Dec 2005)

Defense Critical Infrastructure. (1) DOD and non-DOD networked assets essential to project support and sustain military forces and operations worldwide. (DOD Directive 3020.40 of 19 Aug 2005) (2) Generally consists of physical (installations, power projection platforms, etc.), and nonphysical (electronic information) assets. (JP 3-26) (3) Those systems and assets essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department of Defense to execute the National Military Strategy.

Defense Critical Infrastructure Program. (1) A DOD risk management program that seeks to ensure the availability of networked assets critical to DOD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy. (DODD 3020.40, 19 Aug 2005). (2) A fully integrated program that provides a comprehensive process for understanding and protecting selected infrastructure assets that are critical to national security during peace, crisis, and war. It involves identifying, prioritizing, assessing, protecting, monitoring,

and assuring the reliability and availability of mission-critical infrastructures essential to the execution of the National Military Strategy. (JP 3-26)

Defense Industrial Base (DIB) Sector. The commercial, private sector worldwide industrial complex with capabilities to perform research and development, design, produce and maintain military weaponry systems, subsystems, components or parts to meet military requirements. (DOD Directive 3020.40 of 19 Aug 2005)

Defense Sector. A virtual association within the Defense Critical Infrastructure Program that traverses normal organizational boundaries, encompasses defense networks, assets, and associated dependencies that perform similar functions within the DOD and are essential to the execution of the National Military Strategy. (DOD Directive 3020.40 of 19 Aug 2005)

Financial Services Defense Sector. The DOD, government, and private sector worldwide network and its supporting infrastructure that meet the financial needs of DOD users across the range of military operations. (DODD 3020.40 of 19 Aug 2005)

Global Information Grid (GIG) Defense Sector. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, National Security, and related intelligence community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG also provides interfaces to coalition, allied, and non-DOD users and systems. (Uses existing “GIG”

definition in Joint Publication 1-02, "DOD Dictionary Of Military And Associated Terms," of 12 Apr 2001, as amended through 7 Oct 2004)

Global Information Infrastructure. The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called GII. (JP 3-13, JP 1-02)

Hazard (Infrastructure). Non-hostile incidents such as accidents, natural forces, technological failure, etc., that causes loss or damage to infrastructure assets. (DOD Directive 3020.40 of 19 Aug 2005)

Health Affairs Defense Sector. The DOD, government and private sector worldwide health care network and its supporting infrastructure that meet the health care needs of DOD users across the range of military operations. (DOD Directive 3020.40 of 19 Aug 2005)

Homeland Security Presidential Directive (HSPD)-5. Management of Domestic Incidents. Assigns the Secretary of the Department of Homeland Security as the principal Federal official for domestic incident management to coordinate the Federal Government's resources utilized in response to, or recovery from terrorist attacks, major disasters, or other emergencies. The Federal Government assists state and local authorities when their resources are overwhelmed, or when Federal interests are involved. The Secretary of Defense (SECDEF) provides military support to civil authorities for domestic incidents as directed by the President. SECDEF retains command of military forces providing civil support. Additionally, HSPD-5 established the National Information Management System (NIMS) to provide a consistent nationwide approach for Federal, state, and local governments to work effectively and efficiently together to

prepare for, respond to, and recover from domestic incidents. (JP 3-26)

Homeland Security Presidential Directive (HSPD)-7. Critical Infrastructure Identification, Prioritization and Protection. This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. (HSPD-7 of 17 Dec 2004)

Infrastructure Indications and Warning (I&W). Tactical indications through the implementation of sector monitoring and reporting, strategic indications through Intelligence Community support, and warnings in coordination with the National Infrastructure Protection Center (NIPC) in concert with existing DOD and national capabilities. In infrastructure assurance, indications and warnings may be related to domestic criminal activity, environmental, weather, or technical anomalies that indicate system failure or degradation is likely. Indications are preparatory actions or preliminary infrastructure states that signify that an incident is likely, is planned, or is underway. An official warning would be issued by the responsible organization.

Installation Preparedness. The integration of key activities on DOD installations and facilities that address all efforts pertaining to prevention, detection, protection, response and remediation against all threats and hazards. (DOD Directive 3020.40 of 19 Aug 2005)

Intelligence, Surveillance, and Reconnaissance (ISR) Defense Sector. The DOD, government and private sector worldwide facilities, networks, and systems that conduct and support the collection, production, and dissemination of intelligence, surveillance and reconnaissance information, in support of activities that meet the needs of DOD users across the range of military operations. (DOD Directive 3020.40 of 19 Aug 2005)

Inter-dependency. Relationships or connections between entities of different functions, networks, sectors or services. (DOD Directive 3020.40 of 19 Aug 2005)

Integrated Vulnerability Assessment (IVA). A comprehensive expert third party or peer review, conducted under competent authority, coordination and leadership, synthesizing existing assessment protocols.

International Defense Infrastructure. Elements of international infrastructure that are critical to Department of Defense operations.

Logistics Defense Sector. The DOD, government, and private sector worldwide facilities, networks, and systems that support the provision of supplies and services to U.S. forces. (DOD Directive 3020.40 of 19 Aug 2005)

Military Capability. The ability to achieve a specific wartime objective (win a war or battle, destroy a target set). It includes four major components: force structure, modernization, readiness, and sustainability. (JP 1-02)

Mission Assurance (MA). A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DOD to carry out the National Military Strategy. It links numerous risk management program activities and security related functions—such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—to create the synergistic affect required for DOD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. (DOD Directive 3020.40 of 19 Aug 2005)

Mission Essential Function (MEF). Specified or implied tasks required to be performed by, or derived from, statute or Executive order, and those organizational activities that must be performed under all circumstances to achieve DOD Component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly impact DOD ability to provide vital services, or exercise authority, direction, and control. (DOD Directive 3020.26 of 8 Sep 2004)

Mitigation. Actions taken in response to a warning, or after an incident occurs, that are intended to lessen the potentially adverse effects on a given military operation or infrastructure. (DOD Directive 3020.40 of 19 Aug 2005)

Monitoring and Reporting (M&R). The collection, fusion and dissemination of intelligence-based indications and warnings, DOD asset and civil infrastructure readiness reporting, law enforcement information, man-made or natural hazards, and suspicious security event reporting, that can adversely impact mission readiness. (DOD Directive 3020.40 of 19 Aug 2005)

Network. A group or system of interconnected or cooperating entities, normally characterized as being nodes (assets), and the connections that link them. (DOD Directive 3020.40 of 19 Aug 2005)

Personnel Defense Sector. The DOD, government, and private sector worldwide network that coordinates and support personnel and human resource functions of DOD personnel. (DOD Directive 3020.40 of 19 Aug 2005)

Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02)

Presidential Decision Directive/NSC-63. The statement of National intent to protect infrastructures, both cyber and physical, deemed critical to sustainment of the American way of life. (PDD-63, 22 May 1988)

Public Works Defense Sector. The DOD, government, and private sector worldwide network, including the real property inventories (environment, land, buildings, and utilities), that manages the support, generation, production, and transport of commodities (e.g., electric power, oil and natural gas, water and sewer, emergency services, etc.) for and to DOD users. (DOD Directive 3020.40 of 19 Aug 2005)

Reconstitution. The ability of an agency to recover from a catastrophic event and consolidate the necessary resources that allow it to return to a fully functional entity of the federal government. (Federal Preparedness Circular 65)

Remediation. Actions taken to correct known deficiencies and weaknesses. These actions are undertaken once vulnerability has been identified. (DOD Directive 3020.40 of 19 Aug 2005)

Response. Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include: applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice. (National Response Plan – Homeland Security Dec 2004)

Risk. Probability and severity of loss linked to threats or hazards. (DOD Directive 3020.40 of 19 Aug 2005)

Risk Assessment. A systematic examination of risk using disciplined processes, methods and tools. It provides an environment for decision making to continuously evaluate and prioritize risks and recommend strategies to remediate or mitigate those risks. (DOD Directive 3020.40 of 19 Aug 2005)

Risk Management. A process by which decision makers accept, reduce, or offset risk. (DOD Directive 3020.40 of 19 Aug 2005)

Space Defense Sector. The DOD, government, and private sector worldwide network, including both space- and ground-based systems and facilities, that support launch, operation, maintenance, specialized logistics, control systems, etc., for DOD users. (DOD Directive 3020.40 of 19 Aug 2005)

Subject Matter Expert (SME). An individual who thoroughly understands a business process or area, and is capable of answering detailed questions from others.

Threat. An adversary having the intent, capability and opportunity to cause loss or damage. (DOD Directive 3020.40 of 19 Aug 2005)

Transportation Defense Sector. The DOD, government, and private sector worldwide network that provides U.S. military lift support (surface, sea, and air) for military operations. (DOD Directive 3020.40 of 19 Aug 2005)

Vulnerability (Infrastructure). The characteristics of an installation, system, asset, application, or its dependencies, that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. (DOD Directive 3020.40 of 19 Aug 2005)

Vulnerability Assessment (Infrastructure). A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies, to identify vulnerabilities. (DOD Directive 3020.40 of 19 Aug 2005)

CRITICAL INFRASTRUCTURE PROTECTION COUNCIL MEMBERS

Under Secretary of the Navy

Department of the Navy (DON) Critical Infrastructure Assurance Officer (CIAO)

Department of the Navy Deputy Chief Information Officer (CIO) for Policy and Integration

Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RDA))

Assistant Secretary of the Navy (Financial Management and Comptroller) (ASN (FM&C))

Assistant Secretary of the Navy (Installations and Environment) (ASN (I&E))

Assistant Secretary of the Navy (Manpower & Reserve Affairs) (ASN (M&RA))

Director, Office of Program Appraisal (OPA)

General Counsel (OGC)

Director, Naval Criminal Investigative Service (NCIS)

Assistant for Special Programs and Intelligence, Office of the Under Secretary of the Navy (OUSN (ASP/I))

Commander, Fleet Forces Command (CFFC)

Surgeon General of the Navy (N093)

Director of Naval Intelligence (N2)

Deputy Chief of Naval Operations Information, Plans and Strategy (N3/5)

Director, Information, Plans and Security Division (N3IPS)

Deputy Chief of Naval Operations (Fleet Readiness & Logistics) (N4)

Commander, Navy Installations (CNI)

Deputy Chief of Naval Operations (Warfare, Requirements, and Programs) (N6/7)

Deputy Chief of Naval Operations (Resources, Requirements & Assessments) (N8)

Deputy Commandant, Plans Policies & Operations (USMC PP&O)

The Office of the Naval Inspector General

Commander, Military Sealift Command (MSC)

DEPARTMENT OF THE NAVY CRITICAL INFRASTRUCTURE PROTECTION WORKING GROUP

SECTOR/Contributor	LEAD(S) NAVY/MARINE CORPS
Chair	- Department of the Navy Critical Infrastructure Protection Lead
Service CIP Leads	- Deputy Commmandant Marine Corps Plans, Policies & Operations/Physical Security Division, CIP Branch PP&O/PS PSM - Chief of Naval Operations Staff (OPNAV) Anti-Terrorism/Force Protection Division, Code(N3AT)
Acquisition	- Office of Assistant Secretary of the Navy (Research, Development & Acquisition (ASN (RD&A))
Indications & Warning (Monitoring & Reporting for CIP community)	- Naval Criminal Investigative Service (Multiple Threat Alert Center (MCAT)) - Office of Naval Intelligence
Assessments	- Naval Criminal Investigative Service (Code 21A) - Chief of Naval Operations Staff (OPNAV) Anti-Terrorism/Force Protection Division, Code (N3AT)
Personnel	- Bureau of Naval Personnel/Deputy Chief of Naval Operations, Manpower and Personnel - Deputy Commandant for Manpower and Reserve Affairs
Health Affairs	- Chief of Naval Operations, Director Medical Resources, Plans & Policy Division (N931)
Financial Services	- Deputy Assistant Secretary of the Navy for Financial Operations (FMO)

Logistics	- Director, Supply, Ordnance, Logistics Operations Division (N41) - Deputy Commandant Marine Corps for Installation and Logistics
Transportation	- Director, Supply, Ordnance, Logistics Operations Division (N41) - Military Sealift Command (N34)
Space	- Deputy Chief of Naval Operations Staff (OPNAV) for Warfare Requirements Programs, Space & Communications Pathways Branch (N71)
Defense Information	- Deputy Chief of Naval Operations Staff (OPNAV) for Warfare Requirements Programs, Command, Control, Communications and Computer (C4) Integration & Policy (N098)
Infrastructure/Command, Control, Communications	- Deputy Commandant Marine Corps for Systems Integration (HQMC(C4))
Intelligence, Surveillance, Programs Surveillance, Reconnaissance (ISR)	- Director of Naval Intelligence, Requirements Programs Director, and Reconnaissance Resources & Programs Division (OPNAV N28)
Installations	- Commander, Navy Installations (CNI)
Special Access Programs	- Deputy Chief of Naval Operations (Warfare, Requirements, and Programs) (N7 Special Programs)
Fleet Liaison -	- Commander, Fleet Forces Command
Command Inspections	- The Office of the Naval Inspector General